Bare Demo of IEEEtran.cls for Conferences

Gregory Nazario, Michael Rosen, Lawrence Jackson, Michael Hankowsky
Carnegie Mellon University
Electrical & Computer Engineering
Pittsburgh, USA
{gnazario, mrrosen, lmjackso, mhankows}@andrew.cmu.edu

***Abstract*—SCADA systems are becoming increasingly prevalent, especially wirelessly networked control systems. [citation] The integration of wireless networking into the operation of these SCADA systems is good for many reasons, but these integrations often ignore security as a priority. [citation] Our goal is to better understand the capabilities and the vulnerabilities these systems characteristically possess. In order to do this we will explore the use of cross-layer attacks on networked control systems and develop a framework for testing these attacks. We have developed testbed consists of a simulated network, a simulated factory driven by a matlab-ran Tennessee-Eastman process and the interface between these systems. Our research has confirmed that these vulnerabilities are exploitable and we have established this in our testbed. These vulnerabilities point to the necessity for a change in the way we look at securing SCADA integrated wireless networks.**

I. Introduction

SCADA Systems ... [more on scada]

A. Subsection Heading Here

Subsection text here.

1) Subsubsection Heading Here: Subsubsection text here.

II. Related Work

III. Approach

A. Simulated Network

B. Controller

1) Actuator:

2) Sensor:

3) Internet Cloud:

4) Factory Access Point:

5) Factory Bridge:

C. MATLAB Simulation

We chose to use MATLAB simulation for the physical system and it's controls, as there are many chemical process models currently implemented in MATLAB. This allows for the ease of swapping out current MATLAB models for new ones.

1) Tennessee Eastman: In order to keep the complexity down, we decided to model the chemical process in the plant as a simplified Tenneessee Eastman problem. Due to this approach, we looked to previous work in the field, and found many models already modeled in a hybrid of FORTRAN and MATLAB. However, this introduced more complexity, due to using three different programming languages to implement what should be simpler. Therefore, we would build a custom MATLAB function that contained the same functionality.

D. C++ to MATLAB Bridge

IV. Implementation

A. Simulated Network

1) Controller:

2) Actuator:

3) Sensor:

4) Internet Cloud:

5) Factory Access Point:

6) Factory Bridge:

B. MATLAB Simulation

Our MATLAB

1) Tennessee Eastman: We buit a custom simplified Tennesee Eastman model in MATLAB. This was based off of a preexisting FORTRAN model, but was reimplemented in MATLAB for ease of use and reduced complexity . Our model contains variable vectors, an input vector, a state vector, and an output vector. Then by using the equations provided in Ricker, the simulation simply takes in the input vector from OMNeT++, and outputs the output vector, which includes the sensor data, to OMNeT++ via the MATLAB bridge.

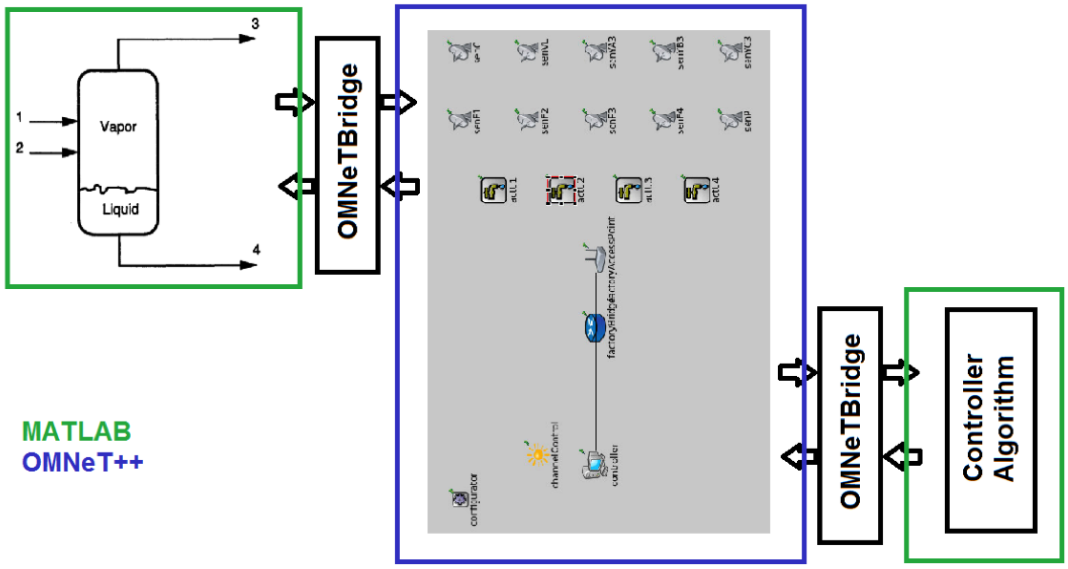

Fig. 1. System Diagram.

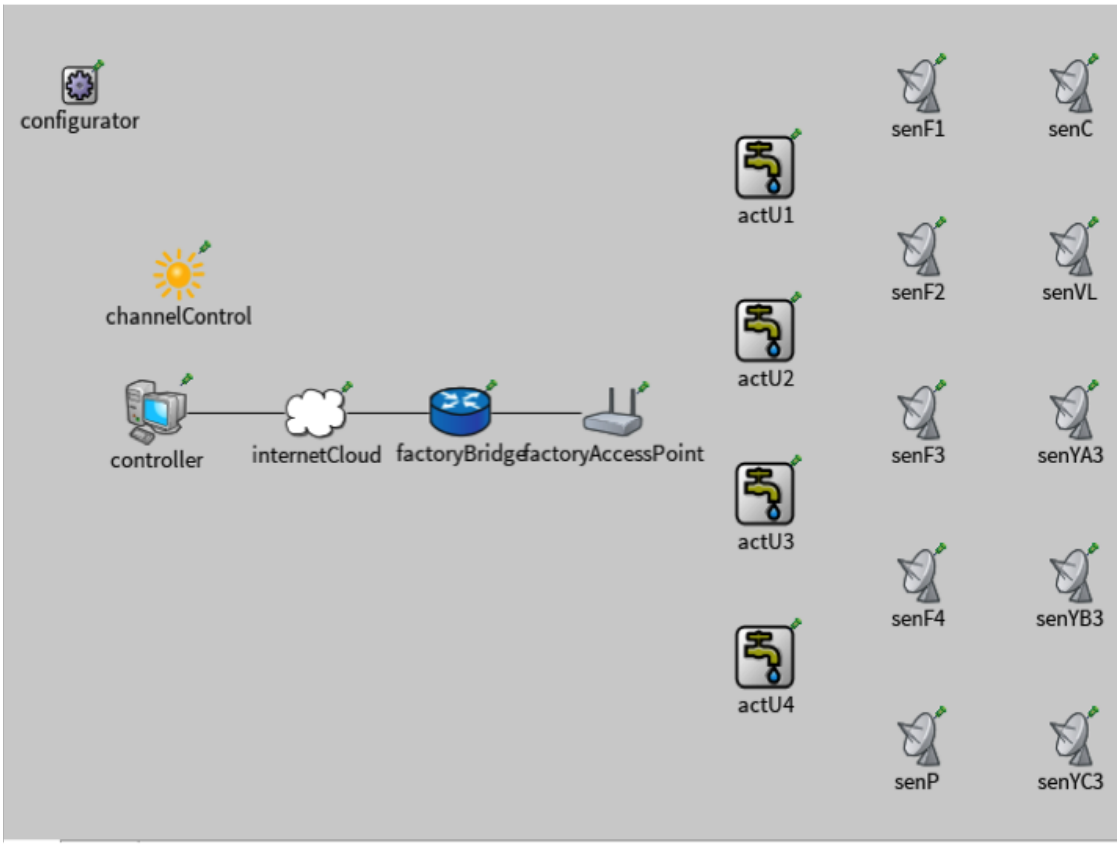

Fig. 2. Network Diagram.

The conclusion goes here.

Acknowledgment

The authors would like to thank...

References

[1] H. Kopka and P. W. Daly, *A Guide to LaTeX*, 3rd ed. Harlow, England: Addison-Wesley, 1999.